# Ingeniería de Software al Servicio de la Informática Forense y la Evidencia Digital

Enrique Miranda[(1)], Hernán Bernardis[(1)], Daniel Riesco[(1)],

[(1)]Departamento de Informática / Facultad Ciencias Físico Matemáticas y Naturales/
Universidad Nacional de San Luis
Ejército de los Andes 950 – San Luis – Argentina
{eamiranda,hbernardis,driesco}@unsl.edu.ar

## Resumen

En los últimos años la Informática Forense, ha demostrado ser una disciplina imprescindible para la aplicación de la ley. Sin embargo, actualmente enfrenta diversos desafíos que requieren del desarrollo de nuevas técnicas y herramientas que posibiliten hacer frente a los mismos. El vertiginoso avance de Internet y la proliferación de dispositivos tecnológicos de uso cotidiano se han convertido en la principal preocupación de los profesionales de la disciplina.

En este contexto de constante demanda, ha surgido una gran cantidad de técnicas y herramientas de software forenses para facilitar la tarea de los profesionales. Sin embargo, es posible distinguir un contexto de crecimiento con cierto déficit en el uso de métodos ingenieriles que faciliten y certifiquen de alguna forma el correcto desarrollo de dichos recursos. Por otra parte, los constantes desafíos requieren de profesionales con cierto grado de formación específica en la temática; aspecto que actualmente no es considerado seriamente por las instituciones de educación superior en nuestro país.

Teniendo en cuenta este contexto se propone una línea de investigación que tome como base los conceptos, técnicas y herramientas de la Ingeniería de Software para asistir a la Informática Forense y al tratamiento de Evidencia Digital.

**Palabras clave**: Informática Forense, Evidencia Digital, Ingeniería de Software, Herramientas Forenses, Educación.

## Contexto

La presente línea de investigación se enmarca en el Proyecto de Investigación "Ingeniería de Software: Conceptos, Prácticas y Herramientas para el Desarrollo de Software con Calidad" de la Facultad de Ciencias Físico Matemáticas y Naturales de la Universidad Nacional de San Luis. Proyecto N° P-031516, continuación de diferentes proyectos de investigación a través de los cuáles se ha logrado vínculos con distintas universidades a nivel nacional e internacional. Además, el mismo se encuentra reconocido por el Programa de Incentivos de Ciencia y Técnica.

## Introducción

Con el avance tecnológico actual estamos viviendo verdaderamente en una era digital. Sin duda alguna este aspecto mejora muchos quehaceres de nuestra vida diaria, al punto tal que no somos verdaderamente conscientes de la cantidad de tareas que realizamos utilizando recursos digitales. Este amplio uso de la tecnología informática en casi todos los ámbitos, sumado al avance revolucionario de las telecomunicaciones, ha favorecido la generación de un "ambiente virtual" en el que se llevan a cabo un sinnúmero de actividades y en donde se almacena un gran volumen de información relacionado a dichas actividades [1,2]. Este tipo de información no ha sido ajena en los procesos penales que se han tenido que adaptarse a este nuevo paradigma conforme fueron evolucionando las distintas conductas llevadas a cabo por medios digitales. En pocas palabras, estamos haciendo referencia a la evidencia digital (o electrónica), que se torna cada vez más esencial y se encamina a convertirse en la prueba fundamental de los procesos penales y de auditorías, posiblemente desplazando con el tiempo en gran medida a la evidencia física [1,4]. Incluso en investigaciones que no son

principalmente de naturaleza digital, en algún momento de la misma pueden surgir elementos de interés en base a archivos o datos informáticos que requieran de un análisis adicional. Es decir, en la actualidad este tipo de evidencia está comenzando a ser un elemento de prueba fundamental en la investigación de cualquier tipo de delito.

La evidencia digital posee ciertas características que la diferencian sobre otras formas de evidencia física. Por ejemplo, la evidencia digital es frágil y volátil, es decir, en ciertos casos la evidencia está almacenada en dispositivo donde cualquier acción puede provocar la alteración de la misma. Además, la evidencia digital se puede copiar *sin límites* de manera relativamente sencilla en la mayoría de los casos. Incluso, el término utilizado es aún más fuerte ya que se habla de "clonación" en vez de copiado ya que el objeto resultante de dicha operación mantiene todas las características del original [1,4]. Otro aspecto no menos relevante acerca de este tipo de evidencia es el volumen de información que normalmente debe ser procesada para la obtención de la misma. Por ejemplo, para lograr obtener una imagen determinada almacenada en un disco rígido de una CPU, es necesario procesar un sinnúmero de archivos que no poseen relevancia. Otra característica es la diversidad de dispositivos en donde se puede almacenar información que puede ser contener evidencia digital. Por ejemplo, discos rígidos, smartphones, drones, dispositivos de IoT, etc.

En este contexto se torna trascendental una disciplina denominada *Informática Forense*, la cual posibilita la detección y recuperación de la información digital que sirva de evidencia a la hora de reconstruir un hecho o sucesión de ellos. La actuación forense en informática permite recuperar y/o reconstruir rastros digitales garantizando su valor probatorio [4].

La Informática Forense requiere de profesionales que cuenten con los conocimientos y la capacitación adecuada para realizar el análisis. En este sentido, los mismos deben demostrar el rigor de las técnicas y herramientas y a su vez deben poder comunicar claramente los resultados a quien corresponda (juez, tribunal, jurado, etc.). Principalmente es por este motivo que los equipos, herramientas y técnicas forenses deben tener su correspondiente validación científica y al mismo tiempo producir un resultado que sea preciso, demostrable y reproducible [1,3].

Para asistir a los profesionales de la Informática Forense existe una amplia variedad de herramientas de software en el mercado, las cuales facilitan, entre otras cosas, la recuperación, análisis y posterior reporte de resultados sobre diversos recursos digitales. Sin embargo, existe una necesidad crítica tanto para las agencias de aplicación de la ley (comúnmente llamadas *law enforcement*) como para las corporaciones de hacer uso estrictamente de herramientas validadas con cierto rigor científico. Frecuentemente los profesionales en Informáticos Forenses hacen uso de herramientas, procedimientos y técnicas que no son accesibles o de público conocimiento para las personas ajenas a la disciplina, por lo tanto, estos no son comprendidos y/o aceptados fácilmente. Para que los hallazgos de un profesional forense sean aceptados, deben ser reconocidos por otros expertos en el campo y cumplir con los estándares de práctica nacionales e internacionales. Los investigadores forenses informáticos corren el riesgo de perder credibilidad si es posible introducir dudas sobre la idoneidad de las herramientas y/o procedimientos desarrollados durante el tratamiento de la evidencia digital presentada [2,4].

Teniendo en cuenta los aspectos relevados anteriormente relacionados con la fiabilidad y la admisibilidad de la evidencia digital, es necesario de común acuerdo entre todos los interesados dentro del proceso, responder algunas cuestiones como por ejemplo qué tipo de herramientas forense de software son las indicadas, cuándo una herramienta de este tipo puede ser utilizada y para qué clase tareas, qué criterios de calidad deben cumplir dichas herramientas, bajo qué requerimientos se debe llevar a cabo una selección, cómo se validan dichas herramientas para que sean "confiables"; por otra parte también es relevante responder a cuestiones como qué conocimientos debe tener ese profesional en Informática Forense para

hacer frente a los desafíos que presenta constantemente la disciplina.

Para dar tratamiento a los cuestionamientos planteados en el párrafo precedente, en esta línea de investigación se propone un abordaje desde la Ingeniería de Software como disciplina de base para facilitar el trabajo forense. Es decir, utilizar conceptos, técnicas, estrategias y herramientas de Ingeniería de Software para afrontar los constantes desafíos que presenta el uso de herramientas de software en Informática Forense para el tratamiento de la Evidencia Digital.

## Líneas de Investigación y Desarrollo

A continuación se describe un conjunto no exhaustivo de temáticas de investigación que se enmarcan dentro de la línea principal.

### Evaluación y Selección de Herramientas de Software Forense

Los planteos más frecuentes en el contexto de la actividad forense están relacionados con la confiabilidad y admisibilidad de la evidencia digital recuperada usando herramientas de software forense [2,3]. Esto ha resaltado la necesidad de que los actores del sistema de justicia respondan y justifiquen de manera precisa preguntas tales como ¿Qué hace que una herramienta de software forense sea aceptada? y ¿Cómo hacer una buena selección de herramientas de software forense? En este contexto, se considera fundamental proporcionar una comprensión más integral de los factores que los profesionales y las empresas de la disciplina consideran importantes para la selección de una herramienta de software forense adecuada [4]. En este sentido es relevante dar respuesta a la siguiente pregunta: ¿Cuáles son los criterios que debe cumplimentar una herramienta de software forense para cada tipo de investigación? La importancia de esta línea de investigación radica en ampliar la comprensión de la selección de herramientas de software forense tomando como base conceptos y prácticas inherentes a la Ingeniería de Software [5,6].

### Validación y Verificación de Herramientas de Software Forense

Uno de los desafíos que enfrentan los profesionales de la Informática Forense es cómo asegurar la confiabilidad (o "solidez forense") de la evidencia digital adquirida por las herramientas utilizadas [7,8]. Actualmente las investigaciones dependen en gran medida de herramientas de software automatizadas. La confiabilidad de los resultados de dichas investigaciones está determinada principalmente por la validación y consistencia de dichas herramientas y su funcionamiento interno. Todos los actores del sistema han planteado una demanda insistente para validar y verificar las herramientas de software forense y así asegurar más la confiabilidad de la evidencia digital [7,8,9].

En esta línea de investigación se propone el estudio y especificación de métodos de verificación y validación de software aplicadas a técnicas y herramientas de Informática Forense.

### Estrategias de Búsqueda y Reducción de Información Digital

Con el paso de los años los dispositivos han adquirido cada vez más capacidad de almacenamiento. A esto se le debe sumar la evolución de internet en una web más compleja donde se pueden encontrar más sitios de almacenamiento en la nube, mayor cantidad de sistemas web de información, base de datos, proliferación de gestores de contenido, etc. Por último, el avance tecnológico ha posibilitado el acceso a una gran variedad de dispositivo a cualquier usuario. De esta manera, cualquier causa a investigar puede involucrar diversos dispositivos con gran capacidad de almacenamiento de datos [4]. Por lo general, a partir del análisis forense de los mismos se extrae gran cantidad de información superflua que no está vinculada con los hechos que se investigan. Este volumen hace más ardua la tarea del profesional forense informático ya que el mismo debe concentrarse en determinar sobre qué tipo de información tiene que hacer foco [10].

En el contexto de análisis de evidencia digital, es necesario contar con técnicas de búsqueda eficiente y reducción de información para poder tratar con el volumen de datos masivo que generalmente resulta de la recuperación forense [10,11,12].

**Modelado e Implementación de Procesos y Herramientas Forenses**

En general, las soluciones existentes en el campo de la Informática Forense son en gran medida *ad-hoc* [5,9]. Dada la importancia de la disciplina y los desafíos y demanda constante en los últimos años, es necesario la especificación de modelos rigurosos de análisis forense y también un desarrollo de procesos y herramientas tomando en cuenta conceptos y técnicas ingenieriles [11,13]. En este sentido, dentro de las ventajas de adoptar este tipo de enfoques, se pueden mencionar: i) un proceso de análisis forense de más amplia aceptación por parte de los actores de la justicia; ii) procesos y herramientas mejores documentados; iii) herramientas más fáciles de mantener y evolucionar; iv) procesos de investigación mejores estructurados; entre otras.

**Técnicas y Herramientas para nuevos Escenarios**

Actualmente la Informática Forense enfrenta muchos desafíos que obligan a buscar y desarrollar nuevas técnicas de análisis de investigación. El desarrollo de dispositivos electrónicos es cada vez más estrepitoso y tiene como objetivo principal llevar los mismos al consumidor de la manera más rápida posible [4].
Dentro de este entorno, la Informática Forense se enfrenta cada vez más a desafíos innumerables, dirigidos principalmente por los nuevos escenarios y tipos de dispositivos que se presentan día a día en el mercado [9,14,15]. Es por esto que se considera fundamental el estudio e implementación de nuevas técnicas y herramientas que permitan hacer frente a este contexto cambiante.

**Educación en Informática Forense y Evidencia Digital**

La demanda de profesionales forenses calificados aumenta constantemente en todo el mundo y Argentina no es la excepción [3,4]. Desde la educación superior se intenta dar solución a los nuevos desafíos que se presentan en la disciplina a nivel científico. Sin embargo desde el aspecto de formación es posible observar que no existe una oferta académica consistente con la amplia demanda. Por otra parte, dentro del grupo de actores relacionados con la disciplina, existen diversas ideas sobre lo que constituye una educación forense adecuada, pero esto no se termina de plasmar en carreras de grado y posgrado; ni siquiera en asignaturas dentro de carreras informáticas. Se puede observar que la oferta de formación está principalmente vinculada a cursos dictados por personas idóneas con buena experiencia en trabajo de campo pero limitada en el ambiente científico-académico.
Por este motivo se considera fundamental abarcar el análisis de un aspecto importante dentro de la disciplina relacionado con la oferta educativa y nuevas estrategias de proliferación de las mismas [16,17]. Esto implica no sólo relevar las opciones de formación para la disciplina en el país, sino también analizar las temáticas excluyentes que debe abarcar dicha formación y finalmente, promover la mejora de la oferta académica tomando como base las instituciones nacionales de educación superior.

## Resultados y Objetivos

Se consolidará un grupo de investigación, desarrollo y transferencia a la comunidad con capacidad para abordar los nuevos desafíos que presentan la Informática Forense y la Evidencia Digital. De esta manera, se plantean como principales objetivos la generación de oportunidades de formación de recursos humanos, desarrollo de oferta académica relativa a la temática, proporción de servicios a la comunidad en el área de estudio, promoción de los vínculos de cooperación con otras instituciones y actores relacionados a la disciplina, entre otros. Con respecto a las líneas

propuestas, se espera: i) estudiar y definir criterios y procesos de evaluación de herramientas de Informática Forense y tratamiento de Evidencia Digital; ii) implementar técnicas de verificación y validación de las herramientas de la disciplina; iii) investigar y unificar las propuestas de la comunidad académica y científica para resolver los distintos desafíos que se plantean en el contexto; iv) definir los criterios de diseño de software que conduzcan a una mejora de las herramientas en general que se utilizan en el entorno v) fomentar el aumento y la mejora de la oferta académica de grado y posgrado relacionado con la temática.

## Formación de Recursos Humanos

Las investigaciones realizadas así como los resultados obtenidos en este trabajo contribuyen al desarrollo de trabajos finales de grado y tesis de posgrado, ya sea de doctorado o maestrías en Ingeniería de Software y desarrollo de trabajos finales de carreras informáticas de la Universidad Nacional de San Luis, en el marco del proyecto de investigación mencionado. Así mismo se pretende que en el corto plazo alumnos de grado y posgrado desarrollen pasantías de investigación y prácticas profesionales en instituciones de aplicación de la ley.

## Bibliografía


[1] DI IORIO, Ana Haydée, et al. El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense. 2017.

[2] ARMILLA, Nicolás, et al. Buenas prácticas para la recolección de la evidencia digital en la Argentina. En *XXIII Congreso Argentino de Ciencias de la Computación, La Plata, 2017*.

[3] CANO, Jeimy. Computación forense descubriendo los rastros informáticos. Editorial: AlfaOmega, México, 2009.

[4] SALT, Marcos. Nuevos desafíos de la evidencia Digital. Acceso transfronterizo y técnicas de acceso remoto a datos informáticos. Editorial: Ad-Hoc, Argentina, 2017.

[5] ARMSTRONG, Colin. Developing a framework for evaluating computer forensic tools. En Evaluation in Crime Trends and justice: Trends and Methods Conference, Canberra Australia. 2003.

[6] RAGHAVAN, Sriram; RAGHAVAN, S. V. A study of forensic & analysis tools. En 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE). IEEE, 2013.

[7] GUO, Yinghua; SLAY, Jill; BECKETT, Jason. Validation and verification of computer forensic software tools - Searching Function. digital investigation, 2009, vol. 6, p. S12-S22.

[8] BECKETT, Jason; SLAY, Jill. Digital forensics: Validation and verification in a dynamic work environment. En 40th Annual Hawaii International Conference on System Sciences, 2007, p. 266a-266a.

[9] WILSDON, Tom; SLAY, Jill. Digital forensics: exploring validation, verification & certification. En First International Workshop on Systematic Approaches to Digital Forensic Engineering, 2005, p. 48-55.

[10] ZOUBEK, Christian; SACK, Konstantin. Selective deletion of non-relevant data. Digital Investigation, 2017, vol. 20, p. S92-S98.

[11] BOGEN, A. Chris; DAMPIER, David A. Preparing for Large-Scale Investigations with Case Domain Modeling. En DFRWS. 2005.

[12] FREILING, Felix; GLANZMANN, Thomas; REISER, Hans P. Characterizing loss of digital evidence due to abstraction layers. Digital Investigation, 2017, vol. 20, p. S107-S115.

[13] BOGEN, A. Chris; DAMPIER, David A. Unifying computer forensics modeling approaches: a software engineering perspective. En First International Workshop on Systematic Approaches to Digital Forensic Engineering, 2005, p. 27-39.

[14] DALINS, Janis; WILSON, Campbell; CARMAN, Mark. Criminal motivation on the dark web: A categorisation model for law enforcement. Digital Investigation, 2018, vol. 24, p. 62-71.

[15] SERVIDA, Francesco; CASEY, Eoghan. IoT forensic challenges and opportunities for digital traces. Digital Investigation, 2019, vol. 28, p. S22-S29.

[16] NANCE, Kara; ARMSTRONG, Helen; ARMSTRONG, Colin. Digital forensics: Defining an education agenda. En 43rd Hawaii International Conference on System Sciences. IEEE, 2010. p. 1-10.

[17] CASEY, Eoghan. What constitutes a proper education? Digital Investigation: The International Journal of Digital Forensics & Incident Response, 2014, vol. 11, no 2, p. 79-80.